

AGENTIC RUNTIME SECURITY

Autonome KI-Handlungen erkennen, kontrollieren und absichern

WER HANDELT UND MIT WELCHEN RECHTEN?

- Wer handelt im Auftrag von wem, wofür und wie lange?
- KI-Agenten lesen Daten, nutzen APIs und führen Aktionen in IT- und OT-Umgebungen aus
- Überprivilegierung, unklare Delegation und langlebige Secrets erhöhen das Risiko

DAS KONTROLLMODELL

Autorisierte Delegation

- Eigene Agentenidentität
- aufgabenbezogener Scope
- kurzlebige Tokens
- widerrufbarer Zugriff

Identität & Secrets

- IBM Verify steuert Identität, Tokens und Policies
- HashiCorp Vault liefert dynamische Credentials
- Audit und Human-in-the-Loop schützen kritische Aktionen

Vom AI-Pilot zum kontrollierten produktiven Betrieb

IHR MEHRWERT: KI SICHER PRODUKTIV SKALIEREN

Mehr Autonomie für KI-Agenten. Volle Kontrolle für Unternehmen.

SICHER SKALIEREN

- Rechte auf Aufgabe, Kontext und Dauer begrenzen
- Kritische Aktionen nachvollziehbar machen und gezielt freigeben
- Identität und Delegation auch über IT-/OT-Grenzen kontrollieren
- NIS2, BSIG, BSI-Grundschutz/B3S und EU AI Act frühzeitig berücksichtigen

WAS SIE GEWINNEN

Weniger Angriffsfläche

- Just-in-Time- und Just-Enough-Access reduzieren überprivilegierte Zugriffe; dynamische Credentials begrenzen Secret Sprawl

Mehr Nachweisbarkeit

- Benutzer-, Agenten- und delegierte Identität bleiben getrennt; Aktionen werden für Revision, Datenschutz und ISMS nachvollziehbar

NÄCHSTER SCHRITT

Agentic Ai Security Quick Check, Architekturworkshop

Bereit für den nächsten Schritt? Im gemeinsamen Gespräch finden wir die passende Strategie. sec@is4it-kritis.de

IHR KONTAKT



MANUEL NOE

Geschäftsführung
mobil +49 171 1496504
email manuel.noe@is4it-kritis.de



MICHAEL FÜHRMANN

Key Account Manager
mobil +49 151 11347223
email michael.fuehrmann@is4it-kritis.de

IS4IT KRITIS GmbH
Kraichgaublick 13
74847 Obrigheim
telefon +49 6262 9262594
www.is4it-kritis.de